<table>
<thead>
<tr>
<th>Article</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The State Administrative Council enacts this Law in accordance with Article 419 of the Constitution of the Republic of the Union of Myanmar.</td>
</tr>
<tr>
<td>2</td>
<td>This Law shall be called the Law Amending the Electronic Transactions Law.</td>
</tr>
</tbody>
</table>
| 3 | Article 2 subsection (a) of the Electronic Transactions Law shall be substituted as follows:  
   (A) “Information” means data, text, images, audio, video, code, software, application, and database. |
| 4 | Article 2 of the Electronic Transactions Law, subsection (k) will be followed by subsection (l), subsection (m), subsection (n), subsection (o), subsection (p), subsection (q) and subsection (r) shall be supplemented as follows:  
   (l) “Personal information” means any information which has been verified or verified as a person associated with a person.  
   (m) “Person responsible for the management of personal information” means the person under any existing law or the provisions of this Law; It means the person and its staff assigned by a government department or organization that has the authority to collect, store, and use personal information. |

---

1 Legislation amending the Electronic Transactions Law

The Republic of the Union of Myanmar
State Administrative Council
State Administrative Council Law No. (7/2021)
Law Amending the Electronic Transactions Law
4th day of the first lunar month, 1382
February 15, 2021
(n) “Management” means the collection of personal information; Acquisition Transfer Distribution; Collaboration; Prohibition Destruction; Recording; Maintenance; Storage; Change Retrieval, advice, and retrieval of archives Use or disclosure.

(o) “Cyber resources” means computers, Computer system; Computer program or program; Network, communication equipment and data.

(p) “Malware” means malicious code that disrupts or endangers a cyber source.

(q) “Cyberspace” means the use of cyber resources in information technology-based networks. Data collection; Electronic information; Computer programs; Software Use electronic applications to access electronic information over a network or network. An environment in which you can send, communicate, distribute, or receive networked or reciprocal networks.

(r) “Cyber-attack” means the use of any cyber resource in the field of cyber’s administrative, financial, economic, Rule of law; Committing an offence against an attack aimed at national security or public safety and property; Attempt to commit; Encouragement; Incitement or conspiracy. (Editor’s note: the corresponding provision in the CSL also referred to provisions which have been removed.)

5. Article 2 of Electronic Transaction Law subsection (l), subsection (m) shall be reclassified as subsection (s), subsection (t), subsection (u).

6. After Article 3 subsection (e), subsection (f) shall be added as follows:

(F) To protect the personal information of the public in accordance with the law.

7. Chapter 10 of the Electronic Transactions Law shall be supplemented as follows:

Chapter (10)
Protection of personal information
27.a. The person responsible for managing and keeping the personal information shall: (Editor’s note: this provision is
(1) systematically keep, protect and manage the personal information based on its types, security levels in accordance with the law

(2) not allow, disclose, inform, distribute, dispatch, modify, destroy, copy and submit as evidence of the personal information of an individual without the consent or the permission in provisions included in an existing law to any individual or organization.

(3) not utilize personal information for managing issues that are not in compliance with the objectives

(4) systematically destroy the personal information that is collected to be used for a period of time after a certain period

27.b. The investigation team who receives information that includes personal information in accordance with the existing laws or the person mandated or instructed on their behalf shall keep the information confidential except disclosing the information in hand in accordance with the law. (Editor’s note: this provision is copied from the draft CSL. Art. 14)

27.c. Personal Information Management shall not include the following: (Editor’s note: this provision is copied from the draft CSL. Art. 15)

1) prevention, search and enquiry, investigation, submission of evidence in regard to cybersecurity, cyber-attacks, cyber-terrorism, cyber misuse and cyber accident, cyber-crimes in a court by the government agency, investigation team or rule of law team assigned by the Central Committee

2) search and enquiry, investigation, collecting information, prosecution and submission of evidence in a court, carried out under the authority of respective criminal case by the government agency, investigation team or rule of law team assigned by the Central Committee.

3) enquiry, investigation, collecting information, coordinating information carried out in accordance with the authority on each relevant issue of stability of state sovereignty, public order, national security [when] the cybersecurity and cybercrime [fall under those aforementioned issues]

4) when carrying out activities in subsection (3),
identification of the management and managing in line with those identifications undertaken by either the central committee or department or organisation assigned by the central committee

8. Chapters (10), (11), (12) and (13) of the Electronic Transactions Law shall be reclassified as Chapters (11), (12), (13) and (14).

9. Article 38-A, 38-B, 38-C, 38-D and 38-E shall be added as follows after Article 38 of the Electronic Transactions Law as follows:

38.a. If a person responsible for managing personal data is convicted of failure to manage personal data in accordance with the provisions under this law, he or she shall be punishable by imprisonment for a term of 1 to 3 years, or a fine not exceeding 100 lakhs, or both.

38.b. Any person, if convicted of obtaining, disclosing, using, destroying, modifying, disseminating or sending personal data of a person to another without approval, shall be punishable by imprisonment for a term of 1 to 3 years, or a fine not exceeding 50 lakhs, or both.

38.c. Any person who is convicted of creating misinformation and disinformation with the intent of causing public panic, loss of trust or social division on cyberspace, shall be punishable by imprisonment for a term of 1 to 3 years, or a fine not exceeding 50 lakhs, or both.

38.d. Any person who is convicted of cyber violence acts such as preventing access to cyber resource or making it difficult; attempting to hack into a cyber source without permission; using more than permitted; and inserting or installing dangerous malware with the intent to hurt someone; with an intent to threaten or disturb national sovereignty, security, peace and stability, rule of law and national solidarity, shall be punished by imprisonment for a term of 2 to 5 years, or a fine not exceeding 300 lakhs, or both.

38.e. Any person who commits acts of cyber-attack such as attempts of unauthorised access to and hacking cyber sources which are kept confidential for nationally, internationally or multilaterally implemented security reasons; and using more than permitted; with the intent of deteriorating the relationship between the country and other foreign countries.
or for the interests of other foreign countries, shall be punished by imprisonment for a term of 3 to 7 years, or a fine not exceeding 700 lakhs, or both.

I sign under Article 419 of the Constitution:

Min Aung Hlaing
Senior General
Chairman
State Administrative Council